



UNITED STATES PATENT AND TRADEMARK OFFICE

50

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------|--------------------------|
| 10/815,222 | 03/31/2004 | Andrew Ginter | VRS-00101 | 7200 |
| 7590 | 06/08/2005 | | | EXAMINER VU, VIET DUY |
| Patent Group Choate, Hall & Stewart Exchange Place 53 State Street Boston, MA 02109-2804 | | | ART UNIT 2154 | PAPER NUMBER |

DATE MAILED: 06/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | |
|------------------------------|------------------------|---------------------|
| Office Action Summary | Application No. | Applicant(s) |
| | 10/815,222 | GINTER ET AL. |
| | Examiner | Art Unit |
| | Viet Vu | 2154 |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 11 April 2005.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 121-166 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 121-166 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5/9/05.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____

Art Unit: 2154

1. The current title is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Art Rejections:

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 121-127, 129-133, 141-148, 150-154 and 162-166 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kronenberg et al, U.S. pat. Appl. Pub. No. 2004/0030778.

Per claims 121-124, Kronenberg discloses a method and system for monitoring an industrial network comprising:

a) providing a plurality of agents for executing at a plurality of computer and control systems in an industrial network (see page 3, par. 46),

b) reporting first data about a first computer system by a first agent executing on the first computer system in the industrial network, the first computer system performing at least one of: monitoring or controlling a physical process of said industrial network such as file monitoring, log file, login, etc., (see page 2, par. 37-39).

Kronenberg does not explicitly teach reporting information about software used in connection with a particular physical process.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to realize such reporting because it would have enabled determining the problem associated with an application, e.g., browser (see page 2, par. 39 and page 5, par. 73).

Per claims 125-127, Kronenberg teaches that the software agent includes a master agent and other agents for performing a set of monitoring tasks (see page 2, par. 38).

Per claims 129-131, Kronenberg teaches monitoring number of connection ports (see page 8, par. 109). It would have been

obvious to one skilled in the art to implement any security rules on the monitored ports.

Per claims 132-133, Kronenberg teaches using rules to process the monitored events (see page 4, par. 52).

Per claim 141, it would have been further obvious to one skilled in the art to utilize any rule on sending the periodical report (see page 6, par. 78).

Claims 142-148, 150-154 and 162-166 are similar in scope as that of claims 121-127, 129-133 and 141.

5. Claims 128, 134-140, 149 and 155-161 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kronenberg and further in view of Schlossberg et al, U.S. pat. Appl. Pub. No. 2002/00660034.

Kronenberg does not explicitly teach handling specific attacking attempts monitored at the security device, e.g., firewall. Schlossberg teaches a network security system for detecting and handling network attacks. Particularly, Schlossberg discloses:

a) detecting suspicious activity in the network (see Schlossberg in page 5, par. 53-54),

b) performing data matching to determine events of interest and assessing a level of threat (see Schlossberg in page 7, par. 63),

c) creating a message for reporting to the management unit,

d) encrypting the message before sending the message (see Schlossberg in page 8, par. 74),

e) decrypting the received message (see Schlossberg in page 7, par. 60 and fig. 7).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kronenberg with Schlossberg's teaching because it would have enabled sufficient handling of network attacks in Kronenberg.

Per claims 135-136 and 156-157, Schlossberg teaches blocking access or shutting down the device, e.g., firewall, in response to an identified attack. (see Schlossberg in page 8, par. 76). It is noted that such changes in operation would reflect on the device configuration.

It would have been further obvious to one of ordinary skill in the art at the time the invention was made to recognize that log data would include any such changes in operation of the device.

Conclusion:

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viet Vu whose telephone number is 571-272-3977. The examiner can normally be reached on Monday through Thursday from 8:00am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee, can be reached on 571-272-3964.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



VIET D. VU
PRIMARY EXAMINER

Art Unit 2154
6/2/05